Central Intelligence Agency

Washington, D.C. 20505

10 NOV 1976

Honorable Abraham Ribicoff, Chairman
Committee on Government Operations
United States Senate
Washington, D. C. 20510

Dear Mr. Chairman:

This is in response to your request for our assistance in the Committee's investigation of the security of computer systems in the Federal Government and subsequent discussions on this subject between representatives of the Agency and Messrs. Fred Asselin and Philip Manuel of your staff.

We share your concerns in the areas of computer security, computer fraud and automated decision-making computer applications. Compromise of a computerized information system can have dire consequences. Fortunately, the fundamental security awareness of the Agency since its inception to protect its operations and its firmly established security concepts and programs formed a solid basis upon which the Agency's security of its computer operations has been built.

A basic underlying maxim is the trustworthiness and integrity of personnel who have access to classified computer systems and to the information contained therein. No measure of technical and physical security will assure protection if the personnel involved are not of proven reliability. This would apply to all persons having access regardless of the level of responsibility. In this regard, the Agency was requested to comment on a statement made by the late Secretary of State Dean Acheson in testimony in 1949 before the Senate Foreign Relations Committee, during a discussion of the espionage threat, that foreign governments concentrate more on compromising low level personnel rather than high level officials. The espionage cases of Sergeants Jack Dunlap and Robert Johnson, who held low level positions, would support this statement and confirm the maxim that all level of positions must be included in any effective security program. Further, when such reliability is established, access to information must be controlled on the basis of strict need-to-know to limit any resultant damage should someone having access later prove to be untrustworthy.

The Agency security concepts and programs for computer security which have evolved and which we offer to the Committee for its consideration are set forth in the enclosure. Our comments are general since, as you undoubtedly understand and appreciate, the Agency cannot for obvious reasons discuss in detail the security methods used to safeguard computer operations. Further, we do not hold ourselves out as a model for other Government agencies, since the degree of protection afforded must be determined by the degree of sensitivity of the information to be protected. Each department and agency responsible for the protection of its information must make its own judgment in this regard.

I trust that this contribution is of some value to the Committee in its deliberations and we appreciate the opportunity to have been of some assistance.

Sincerely,

/s/ George Bush

George Bush

Enclosure

Distribution:
Original - Addressee
1 - DCI
1 - DDCI
1 - ER
1 - Director of Security
1 - ODP
1 - OLC Subject
1 - OLC Chrono
1 - OJCS (Geo. Darnell)
1 - ADP Audit Staff

OLC: PLC: cra (Typed 19 October 1976)
Retyped by dla (4 November 1976)

The authority for the Agency's computer security program is based upon the general authority for the security of the Agency as set forth in statute and Executive Orders. The National Security Act of 1947, (50 U.S.C. 403) Section 102(d)(3) places the responsibility upon the Director of Central Intelligence for the protection of intelligence sources and methods. This responsibility is also expressed in Section 6 of the CIA Act of 1949 (50 U.S.C. 403g). The Agency's program is also governed by the Privacy Act of 1974 (P.L. 94-579) which provides strict guidelines for the proper protection of the storage of personal information and of Executive Order 11652 "Classification and Delcassification of National Security Information and Material" which establishes policy for the protection of classified information. Further, Executive Order 11905, "United States Foreign Intelligence Activities," Section 4(a)(8), establishes the responsibility of the Director of Central Intelligence to provide policy and guidance to the Intelligence Community agencies for the protection of intelligence sources and methods.

The Agency's computer security program was formalized in 1967 as a unique security discipline with the appointment of a Special Assistant for Automatic Data Processing within the Office of the Director of Security. Additional staffing was provided as the Agency's computer operation advanced and grew. At the present time, the Information Systems Security Group of the Office of Security develops and promulgates computer security policy, assists in implementation of this policy and, through a continuing review of computer operations, acts as an enforcement body. The Information Systems Security Group is staffed by both professional security officers and professional data processing personnel. A professional Security officer is also assigned to the Office of Data Processing. This personnel mix provides for the best interchange and understanding of the complex computer security problems and solutions. In addition, this staffing for computer security allows responsiveness to the diversity of computer operations and security requirements.

The Agency's computer security program is a combination of the traditional security concepts of Personnel Security, Physical and Technical Security, and Procedural Security, with Computer Hardware, Software, and Data Security. These concepts and their implementation result in a selection of personnel with high personal integrity combined with procedures establishing legitimate and authorized access and use of the computer and its resources. An underlying

and fundamental goal of the Agency's security program is the protection of information. It should be noted that computer security is but one aspect of the Agency's overall security environment. The computer, as a processor or handler of information, must therefore be protected at the same level as the information it is processing. In addition, high security standards are required because of the storage and availability of large quantities of information within a computer system and the relative ease with which this information can be retrieved and manipulated without appropriate controls.

The unique mission and environment of the CIA have required the establishment of high security standards for all its activities to protect against hostile penetration or destruction. Some specific security features which are supportive for the computer security program are:

a. Personnel

Historically, the Agency has always placed a great deal of emphasis on personnel security. All applicants are subject to a background investigation and polygraph examination to establish that they meet Agency security criteria. These criteria require that all employees be of "excellent character, and of unquestioned loyalty, integrity, discretion and trustworthiness."

Information taken into consideration in determining whether an individual meets these standards is based on, but not limited to, the requirements outlined in Executive Order 10450. In making security clearance determinations, no one event in a person's past is viewed in isolation. The person's entire record is evaluated, and a decision is made based on the totality of that record, rather than on a specific incident which may or may not have been out of character with the rest of this person's conduct. Under these procedures, all personnel hired by the Agency meet the requirements for a Top Secret clearance. This guarantees a high standard of personnel security for all employees used in computer operations by the Agency. Additionally, the Agency has a program under which employees are periodically reinvestigated to confirm that they continue to meet the same high standards as when they entered on duty. A final point is that the Agency personnel security program applies to all employees, no matter what their grade or position. This ensures that there is no one group of employees which is any more vulnerable to security compromise than any other group.

b. Physical Security

The Agency maintains a high degree of physical security protection for all its installations. Physical security can be viewed as protective rings or barriers surrounding an asset. As the value of an asset or, conversely, the assessment of a perceived threat varies, so will the strength of the physical security of the asset. The nature of a computer facility in both value of equipment and data, establishes a high degree of physical security protecting these areas. Examples of physical security features employed are; physical locations, vaulted areas; controlled access, alarms, and established security procedures.

c. Hardware and Software

Computer hardware and the software utilized to operate them have been designed to provide certain forms of self-protection for the computer system and the data stored and processed by them. The Agency employs these protective features, where applicable, as an important and valuable security tool. As evidences of computer vulnerability surface, there is a commensurate demand for security, and the computer hardware and software security features are appropriately emphasized.

d. Security Indoctrination

Security indoctrination and education of all Agency employees is a continuous process. Computer users are additionally provided security indoctrination through briefings, documentation, and notices concerning various computer security problems and features.

In addition to the computer security program at CIA, a group within the ADP Audit Staff, which reports to the Inspector General, was established in 1969. Initially, the attention of this group was focused on automated computer systems in the administrative areas of CIA. Examples of systems of major concern are payroll, general accounting, inventory control, and personnel. As personnel become available, this group plans to extend its audits to other major computer systems in CIA. In addition to periodic reviews of individual systems, the ADP Audit group conducts audits of individual computer installations in CIA to insure proper management controls over computer technology.

Discussions with ADP auditors and managers in private industry and other Government organizations, including GAO, have convinced us that CIA's approach to ADP auditing is correct. The ADP auditor at CIA monitors computer systems during design and development as part of a team. This team includes the end user, the ADP professionals, and the ADP auditor. CIA auditors and ADP professionals agree that it is more difficult and expensive to correct built-in weaknesses after a system is operational than to eliminate the weaknesses in the progressive stages of development and testing.

CIA's program, then, is based on a close working relationship among a group of trained and responsible ADP professionals, an independent group of computer security professionals, and an independent group of ADP auditors. This ongoing program is continually monitored and improved to ensure that it remains effective. CIA is confident that this program provides reasonable safeguards against the computer abuses covered in the recent GAO reports.

Due to its unique mission and environment, the costs of the Agency's security program are accepted as necessary. The computer security program is an integral part of the Agency's overall security program, and it is extremely difficult to cost out this as a separate program other than on a personnel basis. Overall cost factors would, however, at a minimum include personnel clearance, physical security, computer hardware and software, safety and contingency plans, and personnel costs. These specific costs are dependent on the requirements for protection of an asset and its worth.

The Agency's computer security program is based on the value of assets, estimation of the threat to these assets, and a management commitment to protect these assets against threats. The program is not a static one but rather could be described as dynamic, attempting to advance and improve as the computers with which it is involved advance and improve.